



Управление настольными системами

Профессиональные настольные
компьютеры

Номер документа: 361202-251

Май 2004

Данное руководство содержит описания и инструкции по использованию средств защиты и технологии Intelligent Manageability, предварительно установленных на некоторых моделях.

© Компания Hewlett–Packard Development (Hewlett–Packard Development Company, L.P.), 2004.

Информация, содержащаяся в настоящем документе, может быть изменена без предварительного уведомления.

Microsoft и Windows являются охраняемыми товарными знаками корпорации Microsoft в США и других странах.

Все виды гарантий на продукты и услуги компании HP указываются исключительно в заявлениях о гарантии, прилагаемых к указанным продуктам и услугам. Никакие сведения, содержащиеся в данном документе, не должны истолковываться как предоставление дополнительных гарантий. Компания HP не несет ответственности за технические ошибки или опечатки, которые могут содержаться в настоящем документе.

Представленные в данном руководстве сведения защищены законами, регулируемыми отношения авторского права. Никакая часть настоящего руководства не может быть воспроизведена какими-либо средствами (в том числе фотокопировальными) или переведена на другие языки без специального письменного разрешения компании Hewlett–Packard.



ПРЕДУПРЕЖДЕНИЕ. Текст, выделенный таким образом, означает, что невыполнение указаний может привести к травмам или гибели человека.



ОСТОРОЖНО! Текст, выделенный таким образом, означает, что невыполнение указаний может привести к повреждению оборудования или потере данных.

Управление настольными системами

Профессиональные настольные компьютеры

Первая редакция. Май 2004

Номер документа: 361202-251

Содержание

Управление настольными системами

Начальная конфигурация и развертывание	2
Программа удаленной установки системы.	4
Обновление программного обеспечения и управление им	5
Диспетчер HP Client Manager Software	5
Решения Altiris Client Management Solutions.	6
Диспетчер System Software Manager	7
Служебная программа Proactive Change Notification	8
Веб-узел Subscriber's Choice.	8
Флэш-ПЗУ	9
Удаленное изменение данных флэш-ПЗУ	9
Служебная программа HPQFlash	10
Аварийный загрузочный блок ПЗУ	10
Репликация исходной конфигурации настроек компьютера	13
Двухпозиционная кнопка питания	24
Узел Интернета	25
Объединения и партнеры.	25
Средства отслеживания и защиты	26
Защита паролем.	33
Установка пароля на доступ к программе настройки компьютера с помощью программы настройки компьютера	34
Использование пароля на включение питания Программа настройки компьютера	35
DriveLock	41
Датчик снятия крышки	43
Блокировка крышки.	45
Master Boot Record Security (защита главной загрузочной записи).	48
Действия, необходимые перед созданием разделов и форматированием текущего загрузочного диска	51
Замок с тросиком	52
Технология идентификации по отпечаткам пальцев	52

Средства уведомления о сбоях и восстановления	53
Система защиты диска	53
Помехозащищенный блок питания	54
Датчик температуры.	54

Предметный указатель

Управление настольными системами

Система HP Intelligent Manageability обеспечивает базирующиеся на отраслевых стандартах решения управления настольными компьютерами, рабочими станциями и переносными компьютерами, объединенными в сеть. С введением в производство в 1995 году первых полностью управляемых настольных персональных компьютеров компания Hewlett–Packard стала первооткрывателем в области управляемости настольных систем. Компания Hewlett–Packard получила патент на технологию управления HP Intelligent Manageability и с этого момента Hewlett–Packard является лидером отрасли в области развития стандартов и инфраструктур, необходимых для эффективного проведения работ по развертыванию, настройке и управлению настольными компьютерами, рабочими станциями и переносными компьютерами. Компания Hewlett–Packard работает в тесном сотрудничестве с ведущими компаниями отрасли, предлагающими программные решения по управлению, с целью обеспечения совместимости между системой Intelligent Manageability и этими продуктами. Система управления компьютером Intelligent Manageability является важным элементом выполнения взятых нашей компанией на себя обязательств по обеспечению необходимых на протяжении всего периода службы настольного персонального компьютера решений, помогающих осуществлять контроль на всех четырех фазах рабочего цикла — планировании, развертывании, управлении и переходе.

Система обладает следующими основными средствами и возможностями по управлению настольными компьютерами.

- Начальная конфигурация и развертывание
- Удаленная установка системы
- Обновление программного обеспечения и управления им
- Флэш-ПЗУ
- Средства отслеживания и защиты
- Уведомления о неисправностях и средства восстановления



Поддержка тех или иных функций, описанных в этом руководстве, может варьироваться в зависимости от модели или версии программного обеспечения.

Начальная конфигурация и развертывание

Компьютер поставляется с предварительно установленным на нем образом системного программного обеспечения. После непродолжительного процесса «распаковки» программного обеспечения персональный компьютер готов работе.

Можно заменить предустановленный образ программного обеспечения своим вариантом операционной системы и программных приложений. Имеется несколько способов развертывания пользовательского образа программного обеспечения. Они включают:

- Установка дополнительных прикладных программ после «распаковки» предварительно установленной системы программного обеспечения
- Использование программных средств развертывания, таких как Altiris Deployment Solutions™, для замены предустановленного программного обеспечения на пользовательский образ программного обеспечения.
- Использование процесса клонирования дисков для копирования содержимого одного жесткого диска на другой.

Выбор наилучшего метода развертывания зависит от особенностей информационно–вычислительной среды и технологических процессов, реализованных на данном компьютере. Сведения, которые могут помочь выбрать наилучший метод развертывания находятся в разделе «PC Deployment» (развертывание ПК), расположенном на веб–узле Lifecycle Solutions (решения, необходимые на протяжении всего периода службы) по адресу: (<http://whp-sp-orig.extweb.hp.com/country/us/en/solutions.html>).

Компакт–диск *Restore Plus!*, программа установки на основе ПЗУ и оборудование, поддерживающее стандарт ACPI, обеспечивают помощь по восстановлению системного программного обеспечения, управлению конфигурацией и устранению неполадок, а также управлению электропитанием.

Программа удаленной установки системы

Программа удаленной установки системы (Remote System Installation) позволяет осуществлять запуск и установку программного обеспечения, используя для этого находящиеся на сетевом сервере программные средства и конфигурационные данные, активизируемые с помощью предзагрузочной среды выполнения (PXE, Preboot Execution Environment). Это средство обычно применяется для конфигурирования и установки рабочих параметров системы и может использоваться для выполнения следующих операций:

- Форматирование жесткого диска.
- Развертывание образа программного обеспечения на одном или нескольких новых персональных компьютерах.
- Удаленное обновление базовой системы ввода–вывода (BIOS) во флэш–ПЗУ ([«Удаленное изменение данных флэш–ПЗУ» на стр. 9](#)).
- Конфигурирование параметров базовой системы ввода–вывода (BIOS).

Чтобы запустить программу удаленной установки системы (Remote System Installation), нажмите клавишу **F12**, когда в нижнем правом углу экрана с эмблемой Hewlett–Packard появится сообщение «F12 = Network Service Boot» (служба загрузки по сети). Далее следуйте инструкциям на экране. В соответствии с порядком загрузки по умолчанию вначале загружаются параметры конфигурации BIOS. Этот порядок может быть изменен для всех последующих попыток загрузки PXE.

Hewlett–Packard и Altiris объединили свои усилия с целью предоставить программные средства, помогающие сделать задачу развертывания и управления ПК на больших предприятиях и фирмах более легкой и требующей меньше времени, значительно снижающие совокупную стоимость владения и превращающие компьютеры Hewlett–Packard в наиболее легко управляемые клиентские компьютеры в корпоративной среде.

Обновление программного обеспечения и управление им

Hewlett–Packard предоставляет несколько средств управления программным обеспечением для настольных компьютеров и рабочих станций и его обновлением: HP Client Manager Software, Altiris Client Management Solutions, System Software Manager; Proactive Change Notification и Subscriber’s Choice.

Диспетчер HP Client Manager Software

HP Client Manager Software (HP CMS) помогает заказчикам Hewlett–Packard управлять оборудованием на своих клиентских компьютерах с помощью следующих функций:

- Детальный просмотр перечня оборудования для учета имеющихся ресурсов.
- Диагностика и наблюдение за состоянием ПК.
- Заблаговременное уведомление об изменениях в аппаратной среде.
- Сообщение через Интернет о таких критических ситуациях, таких как перегрев компьютера, дефицит памяти и т. п.
- Удаленное обновление программного обеспечения, например, драйверов устройств и системы ввода–вывода (BIOS) ПЗУ.
- Удаленное изменение порядка загрузки

Дополнительные сведения о диспетчере HP Client Manager см. на веб–узле http://h18000.www1.hp.com/im/client_mgr.html.

Решения Altiris Client Management Solutions

HP и Altiris работали как партнеры над созданием полнофункциональных тесно интегрированных решений по управлению системами с целью снижения совокупной стоимости владения клиентскими ПК компании HP. HP Client Manager Software лежит в основе дополнительных решений Altiris Client Management Solutions, которые охватывают:

- Управление инвентаризацией и ресурсами
 - ❑ Соответствие с условиями лицензионного соглашения на программное обеспечение
 - ❑ Отслеживание компьютеров и подготовка отчетов
 - ❑ Отслеживание выполнения условий договора аренды и использования ресурсов
- Развертывание и миграция
 - ❑ Миграция на Microsoft Windows XP Professional или на Microsoft Windows XP Home Edition
 - ❑ Развертывание системы
 - ❑ Миграция личных настроек
- Справочная служба и устранение неполадок
 - ❑ Управление мандатами справочной службы
 - ❑ Дистанционное устранение неисправностей
 - ❑ Дистанционное разрешение проблем
 - ❑ Восстановление систем клиентов после аварий
- Управления программным обеспечением и операционной средой
 - ❑ Текущее управление настольным компьютером
 - ❑ Развертывание системного программного обеспечения компании Hewlett-Packard
 - ❑ Применение средств самовосстановления

Дополнительные более подробные сведения о том, как выполняется загрузка ознакомительной полнофункциональной версии решения Altiris, работоспособной в течение 30 дней, можно получить на веб-узле по адресу:

<http://h18000.www1.hp.com/im/prodinfo.html#deploy>.

На некоторых моделях настольных и переносных компьютеров агент системы управления Altiris включается как часть предварительно загруженного образа программного обеспечения. Данный агент обеспечивает связь с программным обеспечением Altiris Development Solution, которое может использоваться для завершения развертывания нового оборудования или для перемещения индивидуальных настроек в новую операционную систему с помощью простых в использовании мастеров. Решения Altiris предоставляют простые в использовании возможности распространения программ. При использовании этих решений совместно с диспетчером System Software Manager или с диспетчером HP Client Manager Software администраторы могут также обновлять ПЗУ базовой системы ввода-вывода и драйверы устройств с центральной консоли.

Дополнительные сведения см. на веб-узле
<http://h18000.www1.hp.com/im/index.html>.

Диспетчер System Software Manager

Средство System Software Manager (SSM) является программой, позволяющей обновлять программное обеспечение системного уровня одновременно на нескольких компьютерах. При запуске в системе клиентского ПК средство SSM определяет имеющиеся версии программ и устройств, а затем производит обновление соответствующего программного обеспечения из центрального архива данных, известного также под названием «файловое хранилище». Версии драйверов, поддерживаемых диспетчером SSM, содержащиеся на веб-узле загрузки драйверов и на компакт-диске Support Software (программное обеспечение поддержки), помечены специальным значком. Загрузить эту служебную программу и получить дополнительные сведения о диспетчере SSM можно на веб-странице <http://www.hp.com/go/ssm>.

Служебная программа Proactive Change Notification

Программой заблаговременного распространения уведомлений об изменениях (Proactive Change Notification) используется служба Subscriber's Choice, чтобы автоматически и заранее:

- Посылать пользователям по электронной почте уведомления PCN (Proactive Change Notification), заблаговременно (за 60 дней) информируя их об изменениях в оборудовании и программном обеспечении для большинства коммерческих компьютеров и серверов.
- Посылать пользователям по электронной почте сообщения, содержащие выпуски Customer Bulletins, Customer Advisories, Customer Notes, Security Bulletins и Driver Alerts для большинства коммерческих компьютеров и серверов.

Чтобы получать информацию, относящуюся только к своей ИТ-среде, пользователь создает собственный профиль. Получить дополнительные сведения о программе Proactive Change Notification и создать свой собственный профиль можно на веб-узле по адресу:

<http://h30046.www3.hp.com/subhub.php?jumpid=go/pcn>.

Веб-узел Subscriber's Choice

Subscriber's Choice — это клиентская служба HP. Основываясь на профиле пользователя, компания HP будет давать ему индивидуальные рекомендации по продуктам, сообщать о выходящих статьях, а также давать предупреждения и уведомления о драйверах и технической поддержке. Предупреждения и уведомления службы Subscriber's Choice о драйверах и технической поддержке будут рассылать вам по электронной почте уведомления о том, что информация, на которую вы подписались в своем профиле, доступна для просмотра и извлечения. Чтобы получить дополнительные сведения о службе Subscriber's Choice и создать свой профиль, посетите веб-узел <http://h30046.www3.hp.com/subhub.php>.

Флэш-ПЗУ

Компьютер поставляется с программируемым устройством флэш-ПЗУ (постоянным запоминающим устройством). Для защиты ПЗУ от несанкционированного обновления и перезаписи можно установить пароль в служебной программе настройки компьютера (F10). Это важно для обеспечения надежной работы компьютера. При необходимости обновления данных ПЗУ можно выполнить следующие действия:

- Заказать в компании Hewlett-Packard дискету с обновлением — ROMPaq.
- Загрузить последние образы ROMPaq со страницы драйверов и технической поддержки компании HP <http://www.hp.com/support/files>.



ОСТОРОЖНО! Для обеспечения максимального уровня защиты ПЗУ следует убедиться, что установлен пароль для входа в программу настройки компьютера. Этот пароль позволяет предотвратить несанкционированное обновление ПЗУ. Диспетчер System Software Manager позволяет системному администратору установить пароль на одном или нескольких ПК одновременно. Дополнительные сведения см. на веб-узле <http://www.hp.com/go/ssm>.

Удаленное изменение данных флэш-ПЗУ

Возможность удаленного изменения данных флэш-ПЗУ (Remote ROM Flash) позволяет системному администратору безопасно обновлять ПЗУ на удаленных компьютерах Hewlett-Packard непосредственно с центральной консоли управления сетью. Возможность удаленного выполнения этой задачи системным администратором одновременно на нескольких компьютерах позволяет согласовано проводить развертывание образов ПЗУ на находящихся в сети компьютерах Hewlett-Packard и лучше контролировать этот процесс. Это также способствует повышению производительности и снижению затрат на обслуживание.



Для осуществления возможностей удаленного изменения данных флэш-ПЗУ компьютер должен находиться во включенном состоянии или должны быть задействованы средства дистанционного включения компьютера по сети.

Дополнительные сведения об удаленном изменении данных флэш-ПЗУ приводятся в описании диспетчеров HP Client Manager Software и System Software Manager на веб-узле по адресу: <http://h18000.www1.hp.com/im/prodinfo.html>.

Служебная программа HPQFlash

Служебная программа HPQFlash используется для выполнения локального обновления или восстановления системного ПЗУ на персональном компьютере, работающем под управлением операционной системы Windows.

Для получения дополнительных сведений о HPQFlash посетите веб-страницу <http://www.hp.com/support/files> и, в ответ на запрос, введите название компьютера.

Аварийный загрузочный блок ПЗУ

Аварийный загрузочный блок ПЗУ (FailSafe Boot Block ROM) обеспечивает восстановление системы в случае отказа флэш-ПЗУ, например, при отключении питания во время обновления данных ПЗУ. Загрузочный блок представляет собой защищенный от перезаписи раздел ПЗУ, который при включении питания системы находит флэш-ПЗУ, не содержащее ошибок.

- Если системное ПЗУ не содержит ошибок, компьютер загружается как обычно.
- Если происходит сбой системного ПЗУ при проверке, аварийный загрузочный блок ПЗУ позволяет загрузить систему с дискеты ROMPaq, которая перепрограммирует системное ПЗУ по образцу, не содержащему ошибок.



На некоторых моделях предусмотрено восстановление с компакт-диска ROMPaq. Для некоторых моделей образы ISO ROMPaq содержатся в загружаемых пакетах ROM SoftPaqs.

Когда загрузочный блок обнаруживает повреждение системного ПЗУ, индикатор питания мигает красным цветом 8 раз (один раз в секунду) с последующей двухсекундной паузой. Одновременно с этим подается 8 звуковых сигналов. На экране отображается сообщение о переходе в режим восстановления загрузочного блока (на некоторых моделях).

Чтобы восстановить систему после ее входа в режим восстановления загрузочного блока, выполните следующие действия:

1. Если в дисковом гибких дисков или в дисковом компакт-дисков находится носитель, удалите его и выключите питание компьютера.
2. Вставьте дискету ROMPaq в дисковод гибких дисков или, если это возможно на вашем компьютере, компакт-диск ROMPaq в дисковод компакт-дисков.
3. Включите компьютер.

Если определяется отсутствие и дискеты ROMPaq, и компакт-диска ROMPaq, будет выведено сообщение о необходимости вставить дискету или компакт-диск и перезагрузить компьютер.

Если был установлен пароль на вход в программу настройки, загорится индикатор CAPS LOCK и появится запрос на ввод пароля.


4. Введите пароль на вход в программу настройки.

Если система успешно загружается с дискеты и ПЗУ успешно перепрограммируется, на клавиатуре загораются три индикатора. Серия звуковых сигналов повышающегося тона также сообщает об успешном завершении загрузки.

5. Удалите дискету или компакт-диск и выключите питание.
6. Опять включите питание, чтобы перезагрузить компьютер.

В следующей таблице представлены различные сочетания световых сигналов индикаторов клавиатуры, используемые загрузочным блоком ПЗУ (когда к компьютеру подсоединена PS/2–клавиатура), а также значение сигналов и необходимые действия.

Сочетания световых сигналов индикаторов клавиатуры, используемых загрузочным блоком ПЗУ

Режим аварийной загрузки	Цвет индикатора	Клавиатура Действие индикатора	Состояние или сообщение
NUM LOCK	Зеленый	Включено	Носитель (дискета или компакт-диск) ROMPac отсутствует, поврежден или дисковод не готов.
CAPS LOCK	Зеленый	Включено	Введите пароль.
NUM, CAPS, SCROLL LOCK	Зеленый	Мигание световых индикаторов в последовательности — N, C, SL	Клавиатура заблокирована при работе в сетевом режиме
NUM, CAPS, SCROLL LOCK	Зеленый	Включено	Загрузочный блок флэш-ПЗУ успешно завершил работу. Отключите питание и перезагрузитесь
 Диагностические индикаторы не мигают на клавиатурах USB			

Репликация исходной конфигурации настроек компьютера

Описанные ниже процедуры позволяют администратору легко скопировать исходную конфигурацию настроек компьютера на другой компьютер такой же модели. Это позволяет быстро и эффективно настроить несколько компьютеров.



Для выполнения обеих процедур необходим дисковод для гибких дисков или поддержка флэш–устройства USB, например HP Drive Key.

Копирование на один компьютер



ОСТОРОЖНО! Исходные настройки конфигурации зависят от модели компьютера. Репликация настроек конфигурации с одного компьютера на компьютер другой модели может привести к повреждению файловой системы последнего. Например, нельзя копировать настройки конфигурации с настольного компьютера модели dc7100 со сверхплоским горизонтальным корпусом на компьютер с узким вертикальным корпусом модели dx6100.

1. Выберите исходные настройки конфигурации, которые требуется скопировать. Отключите компьютер. В Windows нажмите кнопку **Пуск** и выберите последовательно команды **Завершение работы** и **Завершение работы**.
2. Если используется флэш–устройство USB, вставьте его.
3. Включите компьютер.
4. После включения компьютера нажмите и удерживайте клавишу **F10** до тех пор, пока не будет осуществлен вход в программу управления компьютером. Можно нажать клавишу **ENTER**, чтобы пропустить заставку.



Если своевременно не нажать клавишу **F10**, придется повторно перезагружать компьютер и нажимать и удерживать клавишу **F10**, чтобы получить доступ к программе.

Если используется клавиатура PS/2, можно получить сообщение об ошибке клавиатуры. Не обращайтесь на него внимания.

5. Если используется дискета, вставьте ее.
6. Последовательно выберите **File** (файл), **Replicated Setup** (копируемая конфигурация) и **Save to Removable Media** (сохранить на съемном носителе). Следуйте инструкциям на экране по созданию дискеты или флэш-устройства USB с настройками конфигурации.
7. Выключите компьютер, на который будут переноситься настройки конфигурации, и вставьте в его дисковод дискету или подсоедините к нему флэш-устройство USB с настройками конфигурации.
8. Включите компьютер, на который будут переноситься настройки конфигурации.
9. После включения компьютера нажмите и удерживайте клавишу **F10** до тех пор, пока не будет осуществлен вход в программу управления компьютером. Можно нажать клавишу **ENTER**, чтобы пропустить заставку.
10. Последовательно выберите **File** (файл), **Replicated Setup** (копируемая конфигурация) и **Restore from Removable Media** (восстановить со съемного носителя). Затем следуйте инструкциям на экране.
11. Перезапустите компьютер после завершения настройки его конфигурации.

Копирование на несколько компьютеров



ОСТОРОЖНО! Исходные настройки конфигурации зависят от модели компьютера. Репликация настроек конфигурации с одного компьютера на компьютер другой модели может привести к повреждению файловой системы последнего. Например, нельзя копировать настройки конфигурации с настольного компьютера модели dc7100 со сверхплоским горизонтальным корпусом на компьютер с узким вертикальным корпусом модели dx6100.

В описываемом методе процедура подготовки конфигурационной дискеты или конфигурационного флэш-устройства USB займет несколько больше времени, чем в предыдущем случае, однако процесс копирования на целевой компьютер будет осуществляться значительно быстрее.



Для выполнения данной процедуры требуется загрузочная дискета или загрузочное флэш-устройство USB. Если отсутствует возможность создать загрузочную дискету с помощью Windows XP, следует использовать описанный выше метод копирования на один компьютер (см. «Копирование на один компьютер» на стр. 13).

1. Создайте загрузочную дискету или флэш-устройство USB. См. «Поддерживаемые флэш-устройства USB» на стр. 17 или «Неподдерживаемые флэш-устройства USB» на стр. 20.



ОСТОРОЖНО! Загрузка с помощью флэш-устройства USB может выполняться не на всех компьютерах. Если в служебной программе настройки компьютера (F10) указан порядок загрузки по умолчанию, предусматривающий, что попытка загрузки с флэш-устройства предшествует загрузке с жесткого диска, то загрузка данного компьютера с флэш-устройства USB возможна. В противном случае необходимо будет использовать загрузочную дискету.

2. Выберите исходные настройки конфигурации, которые требуется скопировать. Отключите компьютер. В Windows нажмите кнопку **Пуск** и выберите последовательно команды **Завершение работы** и **Завершение работы**.
3. Если используется флэш-устройство USB, вставьте его.

4. Включите компьютер.
5. После включения компьютера нажмите и удерживайте клавишу **F10** до тех пор, пока не будет осуществлен вход в программу управления компьютером. Можно нажать клавишу **ENTER**, чтобы пропустить заставку.



Если своевременно не нажать клавишу **F10**, придется повторно перезагружать компьютер и нажимать и удерживать клавишу **F10**, чтобы получить доступ к программе.

Если используется клавиатура PS/2, можно получить сообщение об ошибке клавиатуры. Не обращайте на него внимания.

-
6. Если используется дискета, вставьте ее.
 7. Последовательно выберите **File (файл)**, **Replicated Setup** (копируемая конфигурация) и **Save to Removable Media** (сохранить на съемном носителе). Следуйте инструкциям на экране по созданию дискеты или флэш-устройства USB с настройками конфигурации.
 8. Загрузите служебную программу BIOS репликации настройки конфигурации (repset.exe) и скопируйте ее на конфигурационную дискету или флэш-устройство USB. Чтобы получить эту служебную программу, перейдите на веб-страницу <http://welcome.hp.com/support/files> и введите номер модели компьютера.
 9. Создайте на конфигурационной дискете или флэш-устройстве USB файл autoexec.bat, содержащий следующую команду:
repset.exe
 10. Выключите компьютер, на который будут переноситься настройки конфигурации. Вставьте в его дисковод дискету или подсоедините к нему флэш-устройство USB и включите компьютер. Произойдет автоматический запуск служебной программы конфигурации.
 11. Перезапустите компьютер после завершения настройки его конфигурации.

Создание загрузочных устройств

Поддерживаемые флэш-устройства USB

На поддерживаемых устройствах, таких как HP Drive Key или DiskOnKey, имеется заранее установленный образ, упрощающий процесс их превращения в загрузочные. Если на используемом флэш-устройстве USB такой образ отсутствует, следует использовать процедуру, описание которой также будет приведено в данном разделе (см. [«Неподдерживаемые флэш-устройства USB» на стр. 20](#)).



ОСТОРОЖНО! Загрузка с помощью флэш-устройства USB может выполняться не на всех компьютерах. Если в служебной программе настройки компьютера (F10) указан порядок загрузки по умолчанию, предусматривающий, что попытка загрузки с флэш-устройства предшествует загрузке с жесткого диска, то загрузка данного компьютера с флэш-устройства USB возможна. В противном случае необходимо будет использовать загрузочную дискету.

Чтобы создать загрузочное флэш-устройство USB, необходимо иметь:

- Компьютер одной из следующих моделей:
 - ❑ профессиональные настольные компьютеры Hewlett-Packard Compaq серии dc7100;
 - ❑ профессиональные настольные компьютеры Hewlett-Packard Compaq серии dx6100;
 - ❑ профессиональные настольные компьютеры HP Compaq серии d530: со сверхплоским корпусом, с уменьшенным корпусом и с модернизируемым вертикальным корпусом;
 - ❑ настольный компьютер Compaq Evo D510 со сверхплоским корпусом;
 - ❑ компьютер Compaq Evo D510, модернизируемая модель с вертикальным/уменьшенным корпусом;

В зависимости от индивидуальных особенностей системы BIOS будущие модели компьютеров также могут поддерживать загрузку с флэш-устройства USB.



ОСТОРОЖНО! Если используется модель компьютера, не указанная в приведенном выше списке, убедитесь, что в служебной программе настройки компьютера (F10) указан порядок загрузки по умолчанию, предусматривающий, что попытка загрузки с USB-устройства предшествует загрузке с жесткого диска.

- Один из следующих модулей хранения:
 - ☐ 16–мегабайтный модуль HP Drive Key
 - ☐ 32–мегабайтный модуль HP Drive Key
 - ☐ 32–мегабайтный модуль DiskOnKey
 - ☐ 64–мегабайтный модуль HP Drive Key
 - ☐ 64–мегабайтный модуль DiskOnKey
 - ☐ 128–мегабайтный модуль HP Drive Key
 - ☐ 128–мегабайтный модуль DiskOnKey
 - ☐ 256–мегабайтный модуль HP Drive Key
 - ☐ 256–мегабайтный модуль DiskOnKey
- Загрузочную дискету DOS с программами FDISK и SYS. Если на ней отсутствует программа SYS, то может использоваться программа FORMAT, однако в этом случае все файлы, имеющиеся на флэш–устройстве USB, будут утеряны.
 1. Отключите компьютер.
 2. Подсоедините флэш–устройство USB к одному из USB–портов компьютера и отсоедините все другие USB–устройства хранения данных за исключением USB–накопителей гибких дисков.
 3. Вставьте загрузочную дискету DOS с программами FDISK.COM и SYS.COM (или FORMAT.COM) в дисковод и включите компьютер, чтобы выполнить загрузку с загрузочной дискеты DOS.
 4. Запустите программу FDISK, введя после приглашения A:\ **FDISK** и нажав клавишу ENTER. При выводе на экран соответствующего запроса, выберите **Yes (Y)** (да), чтобы включить поддержку больших дисков.

5. Выберите вариант [5], чтобы отобразить накопители компьютера. Флэш-устройству USB будет соответствовать накопитель, указанная емкость которого близка к его фактической емкости. Обычно это последний накопитель в отображаемом списке. Запишите букву, соответствующую имени этого накопителя.

Флэш-устройство USB: _____



ОСТОРОЖНО! Если емкость накопителя не совпадает с емкостью флэш-устройства USB, выполнение описываемой процедуры следует прекратить, поскольку все данные могут быть потеряны. Проверьте все USB-порты на наличие других устройств хранения данных. Если будет обнаружено какое-либо из этих устройств, отсоедините его, выполните перезагрузку компьютера и повторите описываемую процедуру, начиная с шага 4. Если таких устройств не будет обнаружено, то либо данный компьютер не поддерживает флэш-устройство USB, либо это устройство является неисправным. НЕ пытайтесь сделать Drive Key загрузочным устройством.

6. Выйдите из программы FDISK, нажав клавишу **ESC**, чтобы вернуться к приглашению A:\.
7. Если на загрузочной дискете DOS имеется программа SYS.COM, переходите к шагу 8. В противном случае переходите сразу к шагу 9.
8. Введите после приглашения A:\ **SYS x:**, где x соответствует букве имени накопителя, записанной нами на шаге 5.



ОСТОРОЖНО! Убедитесь, в правильности ввода имени накопителя, соответствующего флэш-устройству USB.

После завершения переноса системных файлов, программа SYS возвратится к приглашению A:\. Перейдите к шагу 13.

9. Скопируйте все необходимые файлы с флэш-устройства USB во временную папку на другом диске (например, на внутренний жесткий диск компьютера).

10. Введите после приглашения A:\ **FORMAT /S X:**, где X соответствует букве имени накопителя, записанной нами ранее.



ОСТОРОЖНО! Убедитесь, в правильности ввода имени накопителя, соответствующего флэш-устройству USB.

Программа FORMAT выведет одно или несколько предупреждений, в которых спрашивается, следует ли продолжать выполнение процедуры. Каждый раз в ответ на них необходимо вводить **Y** (да). Программа FORMAT выполнит форматирование флэш-устройства USB, добавит системные файлы и предложит ввести метку тома.

11. Нажмите клавишу **ENTER**, чтобы отказаться от ввода метки или введите ее, если хотите это сделать.
12. Скопируйте все файлы, сохраненные на шаге 9, обратно на флэш-устройство USB.
13. Удалите дискету и выполните перезагрузку компьютера. Компьютер загрузится с устройства флэш-устройства USB, которое отобразится в качестве диска C.



Порядок загрузки по умолчанию на различных компьютерах может быть разным, и может быть изменен с помощью служебной программы настройки компьютера (F10).

При использовании версии DOS из Windows 9x, некоторое время может отображаться экран с эмблемой Windows. Если это нежелательно, добавьте файл нулевого размера с именем LOGO.SYS в корневой каталог флэш-устройства USB.

Возврат на [«Копирование на несколько компьютеров»](#) на стр. 15.

Неподдерживаемые флэш-устройства USB



ОСТОРОЖНО! Загрузка с помощью флэш-устройства USB может выполняться не на всех компьютерах. Если в служебной программе настройки компьютера (F10) указан порядок загрузки по умолчанию, предусматривающий, что попытка загрузки с флэш-устройства предшествует загрузке с жесткого диска, то загрузка данного компьютера с флэш-устройства USB возможна. В противном случае необходимо будет использовать загрузочную дискету.

Чтобы создать загрузочное флэш-устройство USB, необходимо иметь:

- Компьютер одной из следующих моделей:
 - ❑ профессиональные настольные компьютеры Hewlett-Packard Compaq серии dc7100;
 - ❑ профессиональные настольные компьютеры Hewlett-Packard Compaq серии dx6100;
 - ❑ профессиональные настольные компьютеры HP Compaq серии d530: со сверхплоским корпусом, с уменьшенным корпусом и с модернизируемым вертикальным корпусом;
 - ❑ настольный компьютер Compaq Evo D510 со сверхплоским корпусом;
 - ❑ компьютер Compaq Evo D510, модернизируемая модель с вертикальным/уменьшенным корпусом;

В зависимости от индивидуальных особенностей системы BIOS будущие модели компьютеров также могут поддерживать загрузку с флэш-устройства USB.



ОСТОРОЖНО! Если используется модель компьютера, не указанная в приведенном выше списке, убедитесь, что в служебной программе настройки компьютера (F10) указан порядок загрузки по умолчанию, предусматривающий, что попытка загрузки с USB-устройства предшествует загрузке с жесткого диска.

- Загрузочную дискету DOS с программами FDISK и SYS. Если на ней отсутствует программа SYS, то может использоваться программа FORMAT, однако в этом случае все файлы, имеющиеся на флэш-устройстве USB, будут утеряны.

1. Если на компьютере с подключенными накопителями SCSI, ATA RAID или SATA имеются платы PCI, отключите компьютер и отсоедините шнур питания.



ОСТОРОЖНО! Шнур питания ДОЛЖЕН БЫТЬ обязательно отсоединен.

2. Откройте корпус компьютера и удалите все платы PCI.
3. Подсоедините флэш-устройство USB к одному из USB-портов компьютера и отсоедините все другие USB-устройства хранения данных за исключением USB-накопителей гибких дисков. Закройте экран компьютера.
4. Подсоедините шнур питания и включите компьютер.
5. После включения компьютера нажмите и удерживайте клавишу **F10** до тех пор, пока не будет осуществлен вход в программу управления компьютером. Можно нажать клавишу **ENTER**, чтобы пропустить заставку.



Если своевременно не нажать клавишу **F10**, придется повторно перезагружать компьютер и нажимать и удерживать клавишу **F10**, чтобы получить доступ к программе.

Если используется клавиатура PS/2, можно получить сообщение об ошибке клавиатуры. Не обращайтесь к нему.

6. Выберите последовательно **Advanced** (дополнительные) и **PCI devices** (PCI устройства), чтобы отключить контроллеры IDE и SATA. При отключении контроллера SATA запомните номер IRQ, назначенный этому контроллеру. Этот номер потребуется позднее назначить снова. Выйдите из программы настройки, подтвердив сделанные изменения.

SATA IRQ: _____

7. Вставьте загрузочную дискету DOS с программами FDISK.COM и SYS.COM (или FORMAT.COM) в дисковод и включите компьютер, чтобы выполнить загрузку с загрузочной дискеты DOS.
8. Запустите программу FDISK и удалите все имеющиеся на флэш-устройстве USB разделы. Создайте новый раздел и пометьте его в качестве активного. Выйдите из программы FDISK, нажав клавишу **ESC**.

9. Если после выхода из программы FDISK не произойдет автоматической перезагрузки компьютера, нажмите клавиши **CTRL+ALT+DEL**, чтобы выполнить загрузку с дискеты DOS.
10. Введите после приглашения A:\ **FORMAT C: /S** и нажмите клавишу **ENTER**. Программа Format выполнит форматирование флэш-устройства USB, добавит системные файлы и предложит ввести метку тома.
11. Нажмите клавишу **ENTER**, чтобы отказаться от ввода метки или введите ее, если хотите это сделать.
12. Отключите компьютер и отсоедините шнур питания. Откройте корпус компьютера и снова установите удаленные ранее платы PCI. Закройте экран компьютера.
13. Подсоедините шнур питания, удалите дискету и включите компьютер.
14. После включения компьютера нажмите и удерживайте клавишу **F10** до тех пор, пока не будет осуществлен вход в программу управления компьютером. Можно нажать клавишу **ENTER**, чтобы пропустить заставку.
15. Выберите **Advanced** (дополнительные), **PCI devices** (PCI устройства), чтобы снова включить контроллеры PATA и SATA, отключенные ранее на шаге 6. Назначьте контроллеру SATA, его исходный номер IRQ.
16. Сохраните изменения и выйдите из служебной программы. Компьютер загрузится с устройства флэш-устройства USB, которое отобразится в качестве диска C.



Порядок загрузки по умолчанию на различных компьютерах может быть разным, и может быть изменен с помощью служебной программы настройки компьютера (F10). Инструкции см. в *Руководстве по настройке компьютера* на компакт-диске *Documentation CD*.

При использовании версии DOS из Windows 9x, некоторое время может отображаться экран с эмблемой Windows. Если это нежелательно, добавьте файл нулевого размера с именем LOGO.SYS в корневой каталог устройства Drive Key.

Возврат на [«Копирование на несколько компьютеров»](#) на стр. 15.

Двухпозиционная кнопка питания

При включении интерфейса управления питанием (ACPI, Advanced Configuration and Power Interface) кнопка питания может выполнять как функции включения и отключения питания, так и перевода компьютера в ждущий режим. Средство перевода компьютера в ждущий режим не производит полного отключения питания, а переводит компьютер в режим пониженного энергопотребления. Это позволяет быстро понизить энергопотребление компьютера, не закрывая приложений, а затем так же быстро вернуться в исходный рабочий режим без потери данных.

Для изменения функций кнопки питания выполните следующие действия.

1. Нажмите кнопку **Пуск**, затем последовательно выберите **Панель управления** и **Электропитание**.
2. В окне **Свойства: Электропитание** выберите вкладку **Дополнительно**.
3. В разделе **Кнопки питания** выберите **Переход в ждущий режим**.

После установки функций кнопки питания для перехода в ждущий режим для перевода компьютера в режим с очень низким потреблением энергии (ждущий режим) нажмите кнопку питания. Для быстрого возобновления работы компьютера повторно нажмите на кнопку питания. Для полного отключения подачи энергии нажмите и удерживайте кнопку питания в течение четырех секунд.



ОСТОРОЖНО! Используйте кнопку отключения питания компьютера, только если система не отвечает. Выключение питания компьютера без взаимодействия с операционной системой может привести к повреждению или потере данных на жестком диске.

Узел Интернета

Для обеспечения высокой производительности, совместимости и надежности компьютеров Hewlett–Packard инженеры компании осуществляют строгий контроль и отладку программного обеспечения, разработанного компанией Hewlett–Packard и независимыми производителями, а также разрабатывают специальное программное обеспечение.

При переходе на новые или измененные операционные системы необходимо установить программное обеспечение поддержки, разработанное для соответствующей операционной системы. Если планируется использовать версию операционной системы Microsoft Windows, отличающуюся от версии, имеющейся на компьютере, для обеспечения правильной работы всех функций следует установить соответствующие драйверы устройств и служебные программы.

Компания Hewlett–Packard позаботилась о том, чтобы максимально упростить процесс поиска, получения, обновления и установки последних версий программного обеспечения поддержки. Программы можно загрузить с веб–узла <http://www.hp.com/support>.

На веб–узле имеются последние версии драйверов устройств, служебных программ и образы флэш–ПЗУ, необходимые для последней версии операционной системы Microsoft Windows, установленной на данном компьютере Hewlett–Packard.

Объединения и партнеры

Предлагаемые компанией Hewlett–Packard решения по управлению интегрированы с другими приложениями управления компьютером и основываются на таких отраслевых стандартах, как:

- Web–Based Enterprise Management (WBEM)
- Интерфейс управления Windows (WMI)
- Технология Wake on LAN
- Интерфейс ACPI
- Система SMBIOS
- Поддержка предзагрузочной среды выполнения (PXE)

Средства отслеживания и защиты

С помощью средств отслеживания (Asset Tracking), реализованных на данном компьютере, собираются данные для диспетчеров HP Systems Insight Manager, HP Client Manager и для других приложений управления системой. Тесная автоматизированная связь между компонентами средств отслеживания и этими программными продуктами позволяет выбрать средство управления, которое наиболее подходит для данной информационно вычислительной среды и жений в программное обеспечение.

Компания Hewlett-Packard также предлагает различные решения для средств контроля доступа к важным компонентам компьютера и информации. Если установлено устройство встроенной защиты ProtectTools, оно предотвращает несанкционированный доступ к данным, проверяет целостность системы и выявляет попытки посторонних лиц получить доступ к системе. (Дополнительные сведения см. в руководстве *Приступая к работе: диспетчер встроенной системы безопасности ProtectTools компании HP* на компакт-диске *Documentation CD*.) Средства защиты, такие как датчик снятия крышки и блокировка крышки, доступные на некоторых моделях, помогают предотвратить несанкционированный доступ к внутренним компонентам персонального компьютера. Деактивируя параллельный порт, последовательный порт, порт универсальной последовательной шины USB или способность загрузки сменных носителей, можно воспрепятствовать доступу к ценным информационным ресурсам. Сообщения об изменении памяти и предупреждения датчика снятия крышки могут автоматически передаваться приложениям управления системой для обеспечения оперативного уведомления о несанкционированном доступе к внутренним компонентам компьютера.





Такие средства защиты, как датчик снятия крышки и блокировка крышки имеется не на всех компьютерах.

Для управления параметрами защиты компьютеров Hewlett–Packard используйте следующие служебные программы:



- Служебные программы настройки компьютера используются для локального управления. Дополнительные сведения и инструкции по использованию служебных программ настройки компьютера см. в *Руководстве по настройке компьютера (F10)* на компакт–диске *Documentation CD*, входящем в комплект поставки.
- Предлагаемые компанией Hewlett–Packard диспетчеры Client Manager Software и System Software Manager используются для удаленного управления. Эти программные средства обеспечивают надежное и последовательное развертывание, а также управление параметрами защиты с помощью простой служебной программы, запускаемой из командной строки.

В приведенной ниже таблице и последующих разделах объясняется, как локально управлять средствами защиты компьютера, используя служебные программы настройки компьютера (F10).


Обзор средств защиты

Команда	Описание
Setup Password (пароль настройки)	<p>Позволяет устанавливать и включать использование пароля (административного) на доступ к программе настройки компьютера.</p> <p> Если установлен пароль для доступа к программе настройки компьютера, его ввод будет необходим для изменения параметров настройки компьютера, для загрузки новой программы в ПЗУ и изменения некоторых параметров самонастраиваемых (Plug and Play) устройств в Windows.</p> <p>См. руководство <i>Устранение неполадок</i> на компакт-диске <i>Documentation CD</i>.</p>
Power-On Password (пароль на включение компьютера)	<p>Позволяет устанавливать и включать использование пароля на включение питания.</p> <p>См. руководство <i>Устранение неполадок</i> на компакт-диске <i>Documentation CD</i>.</p>
Password Options (уровни защиты) (Эта функция доступна, только если установлен пароль на включение питания.)	<p>Позволяет задавать необходимость ввода пароля при программной перезагрузке (CTRL+ALT+DEL).</p> <p>См. руководство <i>Управление настольными системами</i> на компакт-диске <i>Documentation CD</i>.</p>
Pre-Boot Authorization (предзагрузочная авторизация)	<p>Позволяет включать и отключать использование смарт-карт вместо ввода пароля на включение питания.</p>
	<p>Дополнительные сведения о программе настройки компьютера см. в <i>Руководстве по настройке компьютера (F10)</i> на компакт-диске <i>Documentation CD</i>.</p> <p>Поддерживаемый набор средств защиты может различаться в зависимости от конфигурации компьютера.</p>



Обзор средств защиты (Продолжение)

Команда	Описание
Smart Cover (крышка компьютера)	<p>Позволяет</p> <ul style="list-style-type: none"> • включать или отключать блокировку крышки (Cover Lock). • включать или отключать датчик снятия крышки (Cover Removal Sensor). <p> Уведомление <i>Notify User</i> сообщает пользователю о том, что, по показаниям датчика, крышка компьютера снималась. В режиме <i>Setup Password</i> (пароль для доступа к программе настройки компьютера) для загрузки компьютера требуется ввести пароль для доступа к программе настройки компьютера, если, по показаниям датчика, крышка компьютера снята.</p> <p>Данное средство имеется лишь на некоторых моделях. См. руководство <i>Управление настольными системами</i> на компакт-диске <i>Documentation CD</i>.</p>
Embedded Security (встроенная защита)	<p>Позволяет</p> <ul style="list-style-type: none"> • Включать/выключать устройство встроенной защиты. • Восстанавливать стандартные параметры устройства. <p>Данное средство имеется лишь на некоторых моделях. Дополнительные сведения см. в руководстве «Устройство встроенной защиты <i>ProtectTools</i>» на компакт-диске «Документация»</p>
Device Security (защита устройства)	<p>Включает или выключает последовательные порты, параллельный порт, USB-порты на передней панели, все USB-порты, порты звуковой платы, сетевых контроллеров (на некоторых моделях), MultiBay-устройств (на некоторых моделях) и SCSI-контроллеров (на некоторых моделях).</p>
<p> Дополнительные сведения о программе настройки компьютера см. в <i>Руководстве по настройке компьютера (F10)</i> на компакт-диске <i>Documentation CD</i>.</p> <p>Поддерживаемый набор средств защиты может различаться в зависимости от конфигурации компьютера.</p>	



Обзор средств защиты (Продолжение)

Команда	Описание
Network Service Boot, загрузка сетевой службы	Включение или отключение возможности загрузки на компьютер операционной системы, установленной на сетевом сервере. (Эта функция доступна только в моделях с сетевым адаптером. Сетевой адаптер должен быть подключен к разъему PCI или встроен в системную плату.)
System IDs (идентификаторы компьютера)	<p>Позволяет устанавливать следующие параметры.</p> <ul style="list-style-type: none"> Идентификатор учета (18-байтовый идентификатор) и принадлежности (80-байтовый идентификатор, выводимый на экран во время самотестирования при запуске). <p>Дополнительные сведения см. в руководстве <i>Управление настольными системами</i> на компакт-диске <i>Documentation CD</i>.</p> <ul style="list-style-type: none"> Серийный номер шасси или универсальный уникальный идентификатор UUID (Universal Unique Identifier). Идентификатор UUID можно обновлять только в том случае, если серийный номер шасси неправильный. (Эти идентификационные номера обычно задаются производителем и используются для идентификации компьютера.) <p>Параметры клавиатуры в соответствии с языком страны пользования (например, английским или немецким) для идентификатора компьютера.</p>
<p> Дополнительные сведения о программе настройки компьютера см. в <i>Руководстве по настройке компьютера (F10)</i> на компакт-диске <i>Documentation CD</i>.</p> <p>Поддерживаемый набор средств защиты может различаться в зависимости от конфигурации компьютера.</p>	




Обзор средств защиты (Продолжение)

Команда	Описание
DriveLock	<p>Позволяет назначать или изменять главный или пользовательский пароль для жестких дисков MultiBay (не поддерживается для жестких дисков SCSI). Если это средство включено, в ходе выполнения POST выводится запрос на ввод одного из паролей блокировки диска. Если правильный пароль не будет введен, жесткий диск останется недоступным, пока не будет введен один из нужных паролей во время выполнения последовательности загрузки.</p> <p> Данный параметр отображается только в том случае, когда по крайней мере один жесткий диск MultiBay, поддерживающий блокировку диска, установлен на компьютере.</p> <p>Дополнительные сведения см. в руководстве <i>Управление настольными системами</i> на компакт-диске <i>Documentation CD</i>.</p> <hr/> <p> Дополнительные сведения о программе настройки компьютера см. в <i>Руководстве по настройке компьютера (F10)</i> на компакт-диске <i>Documentation CD</i>.</p> <p>Поддерживаемый набор средств защиты может различаться в зависимости от конфигурации компьютера.</p>

Обзор средств защиты (Продолжение)

Команда	Описание
Master Boot Record Security (защита главной загрузочной записи)	<p>Включение или отключение защиты главной загрузочной записи (MBR).</p> <p>Если защита включена, BIOS блокирует все запросы на изменение MBR на текущем загрузочном диске. При каждом включении или перезагрузке компьютера BIOS сравнивает MBR текущего загрузочного диска с копией, сохраненной ранее. При обнаружении изменений будет предложено три варианта действий: сохранение MBR на текущем загрузочном диске, восстановление предыдущей MBR или отключение защиты MBR. Для этого необходимо знать пароль на доступ к программе настройки (если он был установлен).</p> <p> Перед тем как приступить к разделению или форматированию текущего диска, отключите защиту MBR. Некоторые служебные программы для работы с дисками (такие как FDISK и FORMAT) обновляют MBR.</p> <p>Если защита MBR включена и доступ к диску осуществляется через BIOS, попытки изменения записи MBR пресекаются, в результате служебные программы начинают сообщать об ошибках.</p> <p>Если защита MBR включена и доступ к диску осуществляется через операционную систему, любое изменение MBR будет обнаружено BIOS при следующей загрузке и система защиты MBR выведет соответствующее сообщение.</p>
<p> Дополнительные сведения о программе настройки компьютера см. в <i>Руководстве по настройке компьютера (F10)</i> на компакт-диске <i>Documentation CD</i>.</p> <p>Поддерживаемый набор средств защиты может различаться в зависимости от конфигурации компьютера.</p>	

Обзор средств защиты (Продолжение)

Команда	Описание
Save Master Boot Record (сохранить главную загрузочную запись)	Сохранение резервной копии MBR текущего загрузочного диска. Доступно, только если включена защита MBR.
Restore Master Boot Record (восстановить главную загрузочную запись)	<p>Восстановление MBR текущего загрузочного диска из резервной копии.</p> <p> Доступна только при выполнении следующих условий:</p> <ul style="list-style-type: none"> • включена защита MBR; • ранее была создана резервная копия MBR; • Резервная копия MBR была сделана с текущего загрузочного диска. <p> ОСТОРОЖНО! Восстановление сохраненной ранее MBR после изменения MBR служебной программой или операционной системой может сделать данные на диске недоступными. Восстанавливать MBR из резервной копии следует, только если точно известно, что MBR текущего загрузочного диска испорчена или заражена вирусами.</p>
<p> Дополнительные сведения о программе настройки компьютера см. в <i>Руководстве по настройке компьютера (F10)</i> на компакт-диске <i>Documentation CD</i>.</p> <p>Поддерживаемый набор средств защиты может различаться в зависимости от конфигурации компьютера.</p>	

Защита паролем

Пароль на включение компьютера, препятствующий его несанкционированному использованию, будет затребован каждый раз при включении или повторной инициализации компьютера для дальнейшего доступа к его прикладным программам или содержащейся в его памяти информации. Пароль на доступ к программе настройки препятствует несанкционированному доступу непосредственно к программе настройки и может также использоваться для входа в компьютер вместо пароля на включение компьютера. Таким образом, если вместо затребованного пароля на включение компьютера, будет введен пароль на доступ к программе настройки, все равно будет получен доступ к компьютеру.

Пароль на доступ к программе настройки, действительный для всей сети, позволяет системному администратору зарегистрироваться на любом компьютере сети для проведения обслуживающих работ, не задавая пароля на включение компьютера, даже если таковой был установлен в данной системе.

Установка пароля на доступ к программе настройки компьютера с помощью программы настройки компьютера

Если системе установлено устройство встроенной защиты, см. руководство «*Устройство встроенной защиты ProtectTools*» на компакт-диске «*Документация*». Установка пароля на доступ к программе настройки с помощью программы настройки компьютера предотвращает изменение его конфигурации (использование служебной программы настройки (F10)) без ввода пароля.

1. Включите или перезагрузите компьютер. В Windows нажмите кнопку **Пуск** и выберите последовательно команды **Завершение работы** и **Перезагрузка**.
2. После включения компьютера нажмите и удерживайте клавишу **F10** до тех пор, пока не будет осуществлен вход в программу управления компьютером. Можно нажать клавишу **ENTER**, чтобы пропустить заставку.



Если своевременно не нажать клавишу **F10**, придется повторно перезагружать компьютер и нажимать и удерживать клавишу **F10**, чтобы получить доступ к программе.

Если используется клавиатура PS/2, можно получить сообщение об ошибке клавиатуры. Не обращайтесь на него внимания.

3. Выберите пункт **Security** (защита), затем — **Setup Password** (пароль настройки) и следуйте инструкциям на экране.
4. Перед выходом из программы выберите команду **File** (файл), затем — **Save Changes and Exit** (сохранить изменения и выйти).

Использование пароля на включение питания

Программа настройки компьютера

Установка пароля на включение компьютера с помощью программы настройки компьютера предотвращает доступ к компьютеру при его включении, пока не будет введен пароль. После того как пароль установлен, программа настройки компьютера отображает команду **Password Options** (параметры пароля) в меню **Security** (безопасность). Для параметра пароля можно выбрать значение «**Password Prompt on Warm Boot**» (запрос пароля при перезагрузке). При включенном запросе на ввод пароля при перезагрузке пароль потребуется вводить при каждой перезагрузке компьютера.

1. Включите или перезагрузите компьютер. В **Windows** нажмите кнопку **Пуск** и выберите последовательно команды **Завершение работы** и **Перезагрузка**.
2. После включения компьютера нажмите и удерживайте клавишу **F10** до тех пор, пока не будет осуществлен вход в программу управления компьютером. Можно нажать клавишу **ENTER**, чтобы пропустить заставку.



Если своевременно не нажать клавишу **F10**, придется повторно перезагружать компьютер и нажимать и удерживать клавишу **F10**, чтобы получить доступ к программе.

Если используется клавиатура PS/2, можно получить сообщение об ошибке клавиатуры. Не обращайтесь на него внимания.

3. Выберите пункт **Security** (защита), затем — команду **Power-On Password** (пароль на включение компьютера) и следуйте инструкциям на экране.
4. Перед выходом из программы выберите команду **File** (файл), затем — **Save Changes and Exit** (сохранить изменения и выйти).

Ввод пароля на включение компьютера

Для ввода пароля на включение компьютера выполните следующие действия:

1. Включите или перезагрузите компьютер. В Windows нажмите кнопку **Пуск** и выберите последовательно команды **Завершение работы** и **Перезагрузить компьютер**.
2. Когда на экране монитора появится значок ключа, введите текущий пароль и нажмите клавишу **ENTER**.



Вводите пароль внимательно; так как в целях безопасности вводимые знаки не отображаются на экране.

Если пароль введен неправильно, на экране появится значок сломанного ключа. Попробуйте еще раз. По истечении трех неудачных попыток ввода пароля для продолжения придется выключить и снова включить компьютер.

Ввод пароля на доступ к программе настройки

Если системе установлено устройство встроенной защиты, см. руководство «*Устройство встроенной защиты ProtectTools*» на компакт-диске «*Документация*».

Если для компьютера был задан пароль на доступ к программе настройки, каждый раз при запуске данной программы на экране будет появляться запрос на ввод этого пароля.

1. Включите или перезагрузите компьютер. В Windows нажмите кнопку **Пуск** и выберите последовательно команды **Завершение работы** и **Перезагрузка**.
2. После включения компьютера нажмите и удерживайте клавишу **F10** до тех пор, пока не будет осуществлен вход в программу управления компьютером. Можно нажать клавишу **ENTER**, чтобы пропустить заставку.



Если своевременно не нажать клавишу **F10**, придется повторно перезагружать компьютер и нажимать и удерживать клавишу **F10**, чтобы получить доступ к программе.

Если используется клавиатура PS/2, можно получить сообщение об ошибке клавиатуры. Не обращайтесь к нему.

3. Когда на экране монитора появится значок ключа, введите пароль настройки и нажмите клавишу **ENTER**.



Вводите пароль внимательно; так как в целях безопасности вводимые знаки не отображаются на экране.

Если пароль введен неправильно, на экране появится значок сломанного ключа. Попробуйте еще раз. По истечении трех неудачных попыток ввода пароля для продолжения придется выключить и снова включить компьютер.

Изменение пароля на включение компьютера или на доступ к программе настройки

Если системе установлено устройство встроенной защиты, см. руководство «*Устройство встроенной защиты ProtectTools*» на компакт-диске «*Документация*».

1. Включите или перезапустите компьютер. В Windows нажмите кнопку **Пуск** и выберите последовательно команды **Завершение работы** и **Перезагрузить компьютер**.
2. Чтобы изменить пароль на включение питания, перейдите к шагу 3.

Чтобы изменить пароль для доступа к программе настройки компьютера, сразу после включения компьютера нажмите и удерживайте клавишу **F10** до тех пор, пока не будет осуществлен вход в программу управления компьютером. Можно нажать клавишу **ENTER**, чтобы пропустить заставку.



Если своевременно не нажать клавишу **F10**, придется повторно перезагружать компьютер и нажимать и удерживать клавишу **F10**, чтобы получить доступ к программе.

Если используется клавиатура PS/2, можно получить сообщение об ошибке клавиатуры. Не обращайтесь к нему.

3. При появлении значка ключа введите текущий пароль, косую черту (/) или альтернативный разделитель, затем введите новый пароль, еще одну косую черту (/) или альтернативный разделитель и еще раз новый пароль в следующем порядке:

текущий пароль/новый пароль/новый пароль



Вводите пароль внимательно; так как в целях безопасности вводимые знаки не отображаются на экране.

4. Нажмите клавишу **ENTER**.

Новый пароль действует с момента следующего включения компьютера.



См. «[Национальные разделительные символы клавиатуры](#)» на стр. 40 для получения сведений по альтернативным разделителям. Пароль на включение компьютера и пароль настройки можно также изменять, используя параметры защиты программы настройки компьютера.

Удаление пароля на включение компьютера или пароля настройки

Если системе установлено устройство встроенной защиты, см. руководство «*Устройство встроенной защиты ProtectTools*» на компакт-диске «*Документация*».

1. Включите или перезапустите компьютер. В Windows нажмите кнопку **Пуск** и выберите последовательно команды **Завершение работы** и **Перезагрузить компьютер**.
2. Чтобы удалить пароль на включение питания, перейдите к шагу 3.

Чтобы удалить пароль для доступа к программе настройки компьютера, сразу после включения компьютера нажмите и удерживайте клавишу **F10** до тех пор, пока не будет осуществлен вход в программу управления компьютером. Можно нажать клавишу **ENTER**, чтобы пропустить заставку.



Если своевременно не нажать клавишу **F10**, придется повторно перезагружать компьютер и нажимать и удерживать клавишу **F10**, чтобы получить доступ к программе.

Если используется клавиатура PS/2, можно получить сообщение об ошибке клавиатуры. Не обращайтесь на него внимания.

3. При появлении значка ключа введите текущий пароль, а затем косую черту или альтернативный разделитель, как показано ниже:
текущий пароль/

4. Нажмите клавишу **ENTER**.



См. «[Национальные разделительные символы клавиатуры](#)» для получения сведений по альтернативным разделителям. Пароль на включение компьютера и пароль настройки можно также изменять, используя параметры защиты программы настройки компьютера.

Национальные разделительные символы клавиатуры

Каждая клавиатура разрабатывается в соответствии с конкретными требованиями соответствующей страны. Символы и знаки препинания, которые используются для изменения или удаления пароля, зависят от клавиатуры, которая поставляется вместе с компьютером.

Национальные символы-разделители, используемые на клавиатуре

Арабский	/	Испанский	-	Словацкий	-
БГХСЮ*	-	Итальянский	-	США	/
				(английский язык)	
Бельгийский	=	Канадский	é	Тайский	/
		(французский язык)			
Бразильский	/	Китайский	/	Тайваньский	/
Великобританский	/	Корейский	/	Турецкий	.
Венгерский	-	Латиноамериканский	-	Французский	!
Германский	-	Норвежский	-	Чешский	-
Греческий	-	Польский	-	Шведский/Финский	/
Датский	-	Португальский	-	Швейцарский	-
Израильский	.	Русский	/	Японский	/

* Для Боснии-Герцеговины, Хорватии, Словении и Югославии

Сброс паролей

Если вы забыли свой пароль, доступ к компьютеру будет закрыт. Для получения информации по процедуре сброса паролей обратитесь к *Руководству по устранению неполадок* на компакт-диске *Documentation CD*.

Если системе установлено устройство встроенной защиты, см. руководство «*Устройство встроенной защиты ProtectTools*» на компакт-диске «*Документация*».

DriveLock

Блокировка дисков (DriveLock) — это предусмотренное отраслевым стандартом средство защиты, которое предотвращает несанкционированный доступ к данным на определенных жестких дисках. Блокировка дисков включена в качестве дополнительного средства в программу настройки компьютера. Это средство доступно только в случае обнаружения жестких дисков, поддерживающих функцию DriveLock.

Средство блокировки дисков предназначено для тех клиентов компании Hewlett–Packard, которые в первую очередь заинтересованы в обеспечении безопасности данных. Для таких клиентов затраты на жесткий диск и потеря хранимых на нем данных несопоставимы с тем уроном, который они могут понести в случае несанкционированного доступа к содержимому диска. Чтобы, с одной стороны, обеспечить безопасность такого уровня, а с другой стороны, дать приемлемое решение в случае, когда забыт пароль, в средстве блокировки применяется схема с использованием двух паролей. Один пароль должен быть установлен и использован системным администратором, а другой обычно устанавливается и используется конечным пользователем. Однако если оба пароля забыты, нет никакой возможности разблокировать диск. Поэтому, можно безопасно использовать блокировку диска, только скопировав данные с жесткого диска в корпоративную информационную систему или регулярно создавая резервные копии.

В случае утраты паролей блокировки диска жесткий диск непригоден для дальнейшего использования. Для тех пользователей, которые не относятся к описанной выше категории клиентов, это может оказаться неоправданным риском. Для тех же пользователей, кто относится к упомянутой категории, такой риск может быть вполне обоснован характером данных, хранимых на жестком диске.

Использование функции DriveLock

Параметр DriveLock (блокировка диска) содержится в меню Security (защита) программы настройки компьютера. Здесь предусмотрен ряд параметров, позволяющих устанавливать главный пароль и включать блокировку диска. Чтобы включить блокировку диска, необходим пользовательский пароль. Поскольку начальная конфигурация блокировки диска обычно выполняется системным администратором, главный пароль должен быть установлен первым. Компания Hewlett-Packard рекомендует системным администраторам устанавливать главный пароль в любом случае: собираются они или нет включать блокировку диска. Это даст системным администраторам возможность изменять параметры блокировки диска, если им потребуется впоследствии заблокировать диск. После того как установлен главный пароль, системный администратор может включить блокировку диска или оставить ее отключенной.

Если в системе имеется заблокированный жесткий диск, в ходе проверки POST будет запрошен пароль для снятия блокировки устройства. Если был установлен пароль на включение компьютера и он соответствует пользовательскому паролю на разблокировку устройства, в ходе проверки POST не будет запрашиваться ввод пароля. В противном случае пользователь должен будет ввести пароль блокировки диска. Может использоваться как главный, так и пользовательский пароль. У пользователя есть две попытки для ввода правильного пароля. Если ни одна из попыток не будет успешной, проверка POST будет продолжена, но диск останется недоступным.

Приложения блокировки диска

Лучше всего использовать средства защиты жесткого диска в корпоративной среде, где системный администратор обеспечивает пользователям возможность использовать жесткие диски Multibay на некоторых компьютерах. Системный администратор отвечает за конфигурацию жестких дисков Multibay, для которых, помимо всего прочего, будет установлен главный пароль блокировки диска. В случае если пользователь забудет пользовательский пароль или оборудование будет передано другому сотруднику, всегда можно использовать главный пароль для переустановки пользовательского пароля и получения доступа к жесткому диску.

Компания Hewlett–Packard рекомендует тем системным администраторам, которые решили включить блокировку диска, разработать также корпоративную политику по установке и эксплуатации главных паролей. Это необходимо для того, чтобы предотвратить возникновения ситуаций, когда сотрудники намеренно или непреднамеренно устанавливают оба пароля на блокировку диска перед тем, как уйти из компании. В таких случаях жесткий диск окажется полностью непригодным к использованию, и его придется заменить. Аналогично при отсутствии главного пароля системные администраторы могут оказаться лишены доступа к жесткому диску и не смогут выполнять обычную проверку наличия несанкционированного программного обеспечения, а также другие функции по контролю и поддержке.

Пользователям, у которых нет особых требований к безопасности данных, компания Hewlett–Packard не рекомендует включать блокировку диска. К этой категории относятся частные лица и те пользователи, которые, как правило, не держат на жестком диске секретные данные. Для этих пользователей потенциальная потеря жесткого диска в случае, если они забудут оба пароля, значит гораздо больше, чем те данные, для защиты которых предназначено средство блокировки диска. Доступ к программе настройки и средству блокировки диска может быть закрыт с помощью пароля настройки. Задав пароль настройки и не сообщая его пользователям, системные администраторы могут предотвратить включение пользователями блокировки диска.

Датчик снятия крышки

Датчик снятия крышки (CoverRemoval Sensor), имеющийся на некоторых моделях, использует аппаратные и программные средства, которые позволяют предупреждать о снятии крышки или боковой панели компьютера. Существует три уровня защиты, описанные в следующей таблице.

Уровни защиты, предусмотренные датчиком снятия крышки

Уровень	Параметр	Описание
Уровень 0	Disabled (отключен)	Датчик снятия крышки отключен (по умолчанию).
Уровень 1	Notify User (уведомление пользователя)	Во время перезагрузки компьютера на экране отображается сообщение о том, что была снята крышка или боковая панель компьютера.
Уровень 2	Setup Password (пароль настройки)	Во время перезагрузки компьютера на экране отображается сообщение о том, что была снята крышка или боковая панель компьютера. Необходимо ввести пароль настройки, чтобы продолжить.



Данные параметры могут быть изменены с помощью программы настройки компьютера. Дополнительные сведения о программе настройки компьютера см. в *Руководстве по настройке компьютера (F10)* на компакт-диске *Documentation CD*.

Настройка уровня защиты датчика снятия крышки

Чтобы установить уровень защиты датчика снятия крышки, выполните следующие действия.

1. Включите или перезагрузите компьютер. В Windows нажмите кнопку **Пуск** и выберите последовательно команды **Завершение работы** и **Перезагрузка**.
2. После включения компьютера нажмите и удерживайте клавишу **F10** до тех пор, пока не будет осуществлен вход в программу управления компьютером. Можно нажать клавишу **ENTER**, чтобы пропустить заставку.



Если своевременно не нажать клавишу **F10**, придется повторно перезагружать компьютер и нажимать и удерживать клавишу **F10**, чтобы получить доступ к программе.

Если используется клавиатура PS/2, можно получить сообщение об ошибке клавиатуры. Не обращайте на него внимания.

3. Выберите **Security** (безопасность), **Smart Cover** (крышка корпуса), **Cover Removal Sensor** (датчик снятия крышки) и выберите требуемый уровень защиты.
4. Перед выходом из программы выберите команду **File** (файл), затем — **Save Changes and Exit** (сохранить изменения и выйти).

Блокировка крышки

Блокировка крышки компьютера (Smart Cover Lock) представляет собой замок, имеющийся на некоторых компьютерах Hewlett-Packard, управляемый программными средствами. Это устройство предотвращает несанкционированный доступ к внутренним компонентам. Компьютер поставляется со снятой блокировкой Smart Cover Lock.



ОСТОРОЖНО! Для обеспечения максимального уровня блокировки крышки убедитесь, что установлен пароль для входа в программу настройки компьютера. Пароль настройки предотвращает несанкционированный доступ к служебной программе настройки компьютера.



Блокировка крышки имеется не на всех компьютерах.

Включение блокировки крышки

Чтобы активировать и включить блокировку крышки, выполните следующие шаги.

1. Включите или перезагрузите компьютер. В Windows нажмите кнопку **Пуск** и выберите последовательно команды **Завершение работы** и **Перезагрузка**.
2. После включения компьютера нажмите и удерживайте клавишу **F10** до тех пор, пока не будет осуществлен вход в программу управления компьютером. Можно нажать клавишу **ENTER**, чтобы пропустить заставку.



Если своевременно не нажать клавишу **F10**, придется повторно перезагружать компьютер и нажимать и удерживать клавишу **F10**, чтобы получить доступ к программе.

Если используется клавиатура PS/2, можно получить сообщение об ошибке клавиатуры. Не обращайтесь на него внимания.

3. Выберите команду **Security** (защита), затем — **Cover Lock** (блокировка крышки) и установите параметр **Lock** (включена).
4. Перед выходом из программы выберите команду **File** (файл), затем — **Save Changes and Exit** (сохранить изменения и выйти).

Выключение блокировки крышки

1. Включите или перезапустите компьютер. В Windows нажмите кнопку **Пуск** и выберите последовательно команды **Завершение работы** и **Перезагрузка**.
2. После включения компьютера нажмите и удерживайте клавишу **F10** до тех пор, пока не будет осуществлен вход в программу управления компьютером. Можно нажать клавишу **ENTER**, чтобы пропустить заставку.



Если своевременно не нажать клавишу **F10**, придется повторно перезагружать компьютер и нажимать и удерживать клавишу **F10**, чтобы получить доступ к программе.

Если используется клавиатура PS/2, можно получить сообщение об ошибке клавиатуры. Не обращайтесь на него внимания.

3. Выберите команду **Security** (защита), затем — **Cover Lock** (блокировка крышки) и установите параметр **Unlock** (отключена).
4. Перед выходом из программы выберите команду **File** (файл), затем — **Save Changes and Exit** (сохранить изменения и выйти).

Дополнительный ключ блокировки крышки

Если при включенной блокировке крышки (Smart Cover Lock) ввод пароля для разблокирования невозможен, для открытия крышки компьютера необходим аварийный ключ FailSafe. Этот ключ может потребоваться в следующих ситуациях.

- Отключение электроэнергии
- Сбой при запуске
- Сбой компонента компьютера (например, процессора или блока питания)
- Забыт пароль



ОСТОРОЖНО! Дополнительный ключ является специальным инструментом, поставляемым компанией Hewlett-Packard. Рекомендуется заказать этот ключ заблаговременно у поставщика услуг или уполномоченного представителя.

Для получения ключа выполните одно из следующих действий.

- Обратитесь к уполномоченному представителю Hewlett-Packard или поставщику услуг.
- Обратитесь по телефону (список телефонных номеров содержится в документе о предоставлении гарантии).

Дополнительные сведения об использовании дополнительного ключа блокировки крышки см. в *Справочном руководстве по работе с оборудованием*. на компакт-диске *Documentation CD*.

Master Boot Record Security (защита главной загрузочной записи)

Главная загрузочная запись (MBR, The Master Boot Record) содержит сведения, необходимые для успешной загрузки диска и доступа к данным, которые на нем хранятся. Средство защиты главной загрузочной записи обнаруживает несанкционированные или умышленные изменения MBR, которые могут быть вызваны компьютерными вирусами или неправильным использованием некоторых служебных программ, и сообщает о таких изменениях. Оно также позволяет восстанавливать последнюю не содержавшую ошибок запись MRB, в случае обнаружения изменений в MBR при перезапуске компьютера.

Чтобы включить защиту MBR, выполните следующие шаги.

1. Включите или перезагрузите компьютер. В Windows нажмите кнопку **Пуск** и выберите последовательно команды **Завершение работы** и **Перезагрузка**.
2. После включения компьютера нажмите и удерживайте клавишу **F10** до тех пор, пока не будет осуществлен вход в программу управления компьютером. Можно нажать клавишу **ENTER**, чтобы пропустить заставку.



Если своевременно не нажать клавишу **F10**, придется повторно перезагружать компьютер и нажимать и удерживать клавишу **F10**, чтобы получить доступ к программе.

Если используется клавиатура PS/2, можно получить сообщение об ошибке клавиатуры. Не обращайтесь на него внимания.

3. Выберите команду **Security** (защита), затем — **Master Boot Record Security** (защита главной загрузочной записи) и установите вариант **Enabled** (включено).
4. Выберите команду **Security** (защита), затем — **Save Master Boot Record** (сохранить главную загрузочную запись).
5. Перед выходом из программы выберите команду **File** (файл), затем — **Save Changes and Exit** (сохранить изменения и выйти).

При включенной защите MBR система ввода-вывода (BIOS) предотвращает любые изменения, которые производятся в MBR на текущем загрузочном диске при работе в MS-DOS или в режиме Windows Safe Mode.



В большинстве операционных систем контролируется доступ к MBR на текущем загрузочном диске; BIOS не позволяет предотвратить изменения, которые могут произойти при запуске операционной системы.

При каждом включении или перезагрузке компьютера при работе системы BIOS сравнивается MBR текущего загрузочного диска с копией, сохраненной ранее. Если будут найдены изменения и будет обнаружено, что текущий загрузочный диск является тем самым, на котором была сохранена предыдущая MBR, отобразится следующее сообщение:

1999 — Master Boot Record has changed (1999 — главная загрузочная запись изменилась).

Нажмите любую клавишу для входа в программу настройки и настройки защиты MBR.

После входа в программу настройки компьютера необходимо выполнить следующие действия:

- сохранить MBR текущего загрузочного диска,
- восстановить ранее сохраненную MBR, или
- отключить средство защиты MBR.

Для этого необходимо знать пароль на доступ к программе настройки (если он был установлен).

Если будут найдены изменения или текущий загрузочный диск **не** тот, на котором была сохранена предыдущая MBR, отобразится следующее сообщение:

2000 — Master Boot Record Hard Drive has changed
(2000 — главная загрузочная запись жесткого диска изменилась).

Нажмите любую клавишу для входа в программу настройки и настройки защиты MBR.

После входа в программу настройки компьютера необходимо выполнить следующие действия:

- сохранить MBR текущего загрузочного диска; или
- отключить средство защиты MBR.

Для этого необходимо знать пароль на доступ к программе настройки (если он был установлен).

В том случае, если ранее сохраненная MBR была повреждена, отобразится следующее сообщение:

1998 — Master Boot Record has been lost (1998 — главная загрузочная запись утеряна).

Нажмите любую клавишу для входа в программу настройки и настройки защиты MBR.

После входа в программу настройки компьютера необходимо выполнить следующие действия:

- сохранить MBR текущего загрузочного диска; или
- отключить средство защиты MBR.

Для этого необходимо знать пароль на доступ к программе настройки (если он был установлен).

Действия, необходимые перед созданием разделов и форматированием текущего загрузочного диска

Убедитесь, что отключена защита MBR, прежде чем изменять разбиение или форматировать текущий загрузочный диск. Некоторые служебные программы для работы с дисками, такие как FDISK и FORMAT, обновляют MBR. Если защита MBR включена, при изменении разбиения или форматировании диска могут появляться сообщения об ошибках служебной программы или предупреждения средства защиты MBR при следующем включении или перезагрузке компьютера. Чтобы включить защиту MBR, выполните следующие шаги.

1. Включите или перезагрузите компьютер. В Windows нажмите кнопку **Пуск** и выберите последовательно команды **Завершение работы** и **Перезагрузка**.
2. После включения компьютера нажмите и удерживайте клавишу **F10** до тех пор, пока не будет осуществлен вход в программу управления компьютером. Можно нажать клавишу **ENTER**, чтобы пропустить заставку.



Если своевременно не нажать клавишу **F10**, придется повторно перезагружать компьютер и нажимать и удерживать клавишу **F10**, чтобы получить доступ к программе.

Если используется клавиатура PS/2, можно получить сообщение об ошибке клавиатуры. Не обращайтесь на него внимания.

3. Выберите команду **Security** (защита), затем — **Master Boot Record Security** (защита главной загрузочной записи) и установите вариант **Disabled** (отключено).
4. Перед выходом из программы выберите команду **File** (файл), затем — **Save Changes and Exit** (сохранить изменения и выйти).

Замок с тросиком

К задней панели некоторых моделей компьютеров можно присоединить замок с тросиком, позволяющий физически закрепить компьютер на рабочем месте.

Наглядно проиллюстрированные инструкции см. в *Справочном руководстве по работе с оборудованием* на компакт-диске *Documentation CD*.

Технология идентификации по отпечаткам пальцев

Устраняя необходимость ввода паролей конечными пользователями, технология идентификации по отпечаткам пальцев (HP Fingerprint Identification Technology) повышает сетевую безопасность, упрощает процедуру входа в систему и снижает затраты на управление корпоративными компьютерными сетями. Доступная по цене, эта технология предназначена не только для организаций, использующих высокие технологии и имеющих повышенный уровень секретности.



Поддержка технологии идентификации по отпечаткам пальцев варьируется в зависимости от модели.

Дополнительные сведения см. на веб-узле:

<http://h18004.www1.hp.com/products/security/>.

Средства уведомления о сбоях и восстановления

Средства уведомления о сбоях и восстановления совмещают передовые аппаратные и программные технологии и позволяют предотвратить потерю важных данных и свести к минимуму время вынужденного простоя оборудования.

Если компьютер подключен к сети, управляемой с помощью программы HP Client Manager, уведомление о сбое отправляется приложению управления сетью. С помощью программы HP Client Manager Software также можно удаленно планировать выполнение программ диагностики неполадок, обеспечивая их автоматический запуск на всех управляемых ПК и создание сводного отчета непрошедших проверок.

Система защиты диска

Система защиты диска (DPS, Drive Protection System) — это диагностическое средство, встроенное в жесткие диски некоторых настольных компьютеров Hewlett-Packard. Система DPS предназначена для обнаружения неполадок, которые могут привести к негарантийной замене жесткого диска.

При изготовлении компьютеров Hewlett-Packard каждый устанавливаемый жесткий диск проверяется с использованием DPS, и на него записываются специальные нестираемые данные. При каждом применении DPS результаты проверки записываются на жесткий диск. Службы технической службы могут использовать эти данные для определения причины запуска проверки DPS. Сведения по использованию средств DPS содержатся в *Руководстве по устранению неполадок* на компакт-диске *Documentation CD*.

Помехозащищенный блок питания

Встроенный помехозащищенный блок питания обеспечивает повышение надежности работы компьютера при наличии помех в сети питания. Этот блок питания выдерживает импульсные помехи амплитудой до 2000 вольт без каких-либо сбоев в работе компьютера или потери данных.

Датчик температуры

Датчик температуры представляет собой программное средство и компонент оборудования, который следит за внутренней температурой компьютера. Он выводит на экран предупреждение о том, что превышен температурный предел, что позволяет предпринять необходимые действия, прежде чем будут повреждены внутренние компоненты компьютера или утрачены данные.

Предметный указатель

A–Z

Altiris 6
deleting password 39
DiskOnKey
 см. также HP Drive Key
 загрузочное устройство 17 — 23
Drivelock 41 — 43
HP Client Manager 5
HP Drive Key
 см. также DiskOnKey
 загрузочное устройство 17 — 23
Multibay, защита 41 — 43
password
 deleting 39
PCN (Proactive Change Notification) 8
power-on password
 deleting 39
Proactive Change Notification (PCN) 8
PXE — предзагрузочная среда
 выполнения 4
Remote ROM Flash 9
setup password
 deleting 39
Smart Cover Lock 45 — 47
Smart Cover Sensor 43
SSM (System Software Manager) 7
System Software Manager (SSM) 7

A

аварийный загрузочный блок ПЗУ 11
адреса URL (веб-узлы). *см.* веб-узлы

Б

безопасность
 блокировка крышки 45
 дополнительный ключ 47
 защита ПЗУ 9
 параметры, установка 26
 средства защиты, таблица 28
блок питания, помехозащищенный 54
блокировка крышки 45
 включение 45
 выключение 46
блокировка крышки, безопасность 45
блокировка крышки, заказ
 дополнительного ключа 47

В

ввод
 включение компьютера, пароль 36
 пароль настройки 36
веб-узлы
 Altiris 6, 7
 HP Client Manager 5
 HPQFlash 10
 Proactive Change Notification 8
 ROMPaq, образы 9
 Subscriber's Choice 8
 System Software Manager (SSM) 7
 программное обеспечение,
 поддержка 25
 репликация, служебная
 программа 16, 17

- технология идентификации по отпечаткам пальцев 52
- удаленное изменение данных флэш–ПЗУ 10
- Флэш–ПЗУ 9
- включение блокировки крышки 45
- включение компьютера, пароль ввод 36
- изменение 37
- внутри корпуса компьютера, температура 54
- восстановление системы 10
- восстановление, программное обеспечение 3
- выключение блокировки крышки 46

Г

- главная загрузочная запись, защита 48 — 50

Д

- датчик снятия крышки
- настройка 44
- уровни защиты 44
- две функции кнопки питания 24
- диагностические средства для жестких дисков 53
- диск, защита 53
- диск, клонирование 3
- дополнительный ключ
- безопасность 47
- заказ 47
- доступ к компьютеру, контроль 26

Ж

- жесткие диски, диагностические средства 53

З

- загрузочное устройство
- DiskOnKey 17 — 23
- HP Drive Key 17 — 23
- создание 17 — 23
- флэш–устройство USB 17 — 23
- загрузочный диск, важная информация 51
- заказ дополнительного ключа 47
- замок с тросиком 52
- защита
- DriveLock 41 — 43
- MultiBay 41 — 43
- Smart Cover Lock 45 — 47
- Smart Cover Sensor 43
- главная загрузочная запись 48 — 50
- пароль 33
- защита главная загрузочная запись 48 — 50
- защита жестких дисков 53
- защита ПЗУ, безопасность 9

И

- изменение настройки программного обеспечения 3
- изменение операционных систем, важная информация 25
- изменение пароля 37
- изменения, уведомление об 8
- индикаторы клавиатуры, ПЗУ, таблица 12
- Интернет–адреса, см. веб–узлы
- исходная конфигурация настроек
- репликация 13

К

клавиатура, национальные
разделительные символы 40
кнопка питания
настройка 24
кнопка питания с двумя функциями 24
контроль доступа к компьютеру 26

Н

настройка
начальная 2
настройка кнопки питания 24
национальная клавиатура,
разделительные символы 40
начальная конфигурация 2

О

обновление ПЗУ 9
операционные системы, важная
информация 25

П

пароль
включение компьютера 36
защита 33
изменение 37
настройка 34
настройки 36
сброс 40
пароль на настройку
изменение 37
пароль настройки
ввод 36
здание 34
ПЗУ
индикаторы клавиатуры, таблица 12
повреждение 11
удаленное изменение данных
флэш-ПЗУ 9
ПЗУ, обновление 9

повреждение системного ПЗУ 11
помехозащищенный блок питания 54
предзагрузочная среда выполнения
(PXE) 4
предустановленный образ
программного обеспечения 3
программное обеспечение
Remote ROM Flash 9
System Software Manager 7
аварийный загрузочный
блок ПЗУ 11
восстановление 3
главная загрузочная запись,
защита 48 — 50
интеграция 3
обновление нескольких
компьютеров 7
система защиты дисков 53
служебные программы копирования
исходных настроек компьютера 13
средства отслеживания 26
уведомление о сбоях
и восстановление 53
удаленная установка системы 4

Р

разбиение диска на разделы,
важная информация 51
разделительные символы, таблица 40

С

сброс пароля 40
система, восстановление 10
Служебные программы копирования
исходных настроек компьютера 13
средства клонирования, программное
обеспечение 3
средства отслеживания 26
средства развертывания, программное
обеспечение 3

Т

температура внутри компьютера 54

температурный датчик 54

технология идентификации по
отпечаткам пальцев 52

У

уведомление о сбоях 53

уведомление об изменениях 8

удаленная установка 4

удаленная установка системы, доступ 4

Ф

флэш-устройство USB,
загрузочное 17 — 23

форматирование диска, важная
информация 51